Transposition Cipher dan *Grille Cipher*

Kevin Wibowo-13509065
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13509065@std.stei.itb.ac.id

Abstraksi— ***Dalam makalah yang akan dibuat akan dibahas salah satu topik dari kriptografi enkripsi klasik yang tampaknya jarang diperhatikan, padahal metode ini cukup kuat. Metode tersebut adalah metode enkripsi transposisi. Metode ini mempunyai dasar yang sangat sederhana yaitu mengubah urutan dari huruf-huruf yang ada, tetapi pendeteksian akan sangat sulit bila tidak mempunyai kuncinya. Metode-metode transposisi juga dapat digabungkan dengan metode lain seperti subtitusi agar pesan menjadi sangat aman. Terdapat berbagai macam metode transposisi seperti*** **columnar transposition, double transposition, Grille cipher,** ***dan lain-lain. Metode*** **Grille Cipher** ***adalah salah satu metode yang bisa digunakan sebagai kriptografi dan juga dapat digunakan untuk steganografi (metode untuk menyembunyikan pesan). Metode ini menggunkan pergeseran tanpa rumus, tetapi menggunakan template posisi pengubahan. Dengan menggunakan template yang tersedia, penyembunyian pesan akan dapat dilakukan dengan mudah. Metode*** **Grille Cipher** ***ini juga mempunyai beberapa variasi seperti*** **single Grille cipher, chessboard Grille,** ***dan masih banyak lagi.***

***Kata Kunci*— Transpotition Cipher, Key, Grille, Plain Text, Cipher Text.**

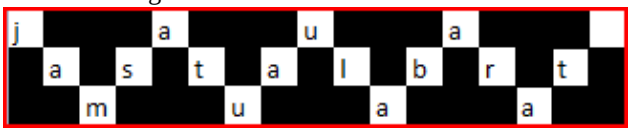
I. TRANSPOSITION CIPHER

Transposition cipher adalah salah satu jenis teknik pengenkripsian pesan dengan cara mengubah urutan huruf-huruf yang ada di dalam *plainteks*(pesan yang belum dienkripsi) menjadi *cipherteks* pesan ynag telah dienkripsi) dengan cara tertentu agar isi dari pesan tersebut tidak dimengerti kecuali oleh orang-orang tertentu. Pada dasarnya prinsip pengubahan pesan mirip dengan anagram seperti kata "melepas" diubah menjadi "saeelpm", tapi tentu saja transposition cipher mempunyai rumus atau kunci tertentu yang diperlukan agar pesan bisa dimengerti. Berikut adalah beberapa contoh transposition cipher.

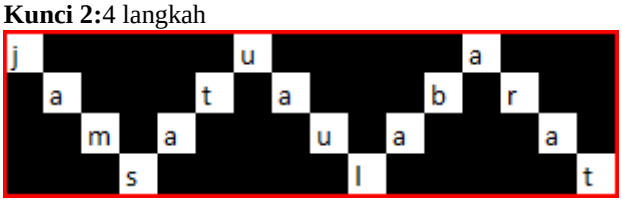
1.1 *Rail Fence Cipher*

Rail Fence cipher adalah salah satu jenis *transposition cipher*, yang menggunakan prinsip seperti rel kereta api yang terdapat dua buah jalur besi dan kayu jembatan ditengah-tengahnya. Dalam *cipher* ini kita menyusuri rel tersebut dengan naik-turun melalui jembatan. Kunci dapat berupa seberapa jauh jembatan kayu tersebut(panjang naik turun). Setelah itu pesan akan dibaca secara mendatar untuk mendapatkan cipherteks.

Contoh:
Plainteks:jam satu aula barat
(putih diisi huruf secara naik turun, hitam kosong)
Kunci 1:3langkah



Kunci 2:4 langkah



Cipherteks1: jauaastalbrtmuaa
Cipherteks2: juaatabrmauaaslt

1.2 *Route Cipher*

Route Cipher adalah salah satu jenis cipher yang merupakan perluasan *rail fence cipher*. Cara ini mirip karena menggunakan rute seperti *rail fence*, tetapi dalam hal ini rute bisa berupa apa saja seperti melingkar kedalam atau rute khusus. Biasanya kunci berupa cara baca. Walaupun memiliki kunci pemecahan cukup memakan waktu dibanding cipher lainnya. Untuk pemecahan dapat dimisalkan dengan angka

Contoh:
Plainteks: jam satu aula barat
Kunci 1:buat 4x4 kotak kosong lalu dari kanan atas tulis melingkar kedalam

l	a	b	j
u	t	a	a
a	a	r	m
u	t	a	s

Kunci 2:buat 4x4 kotak lalu dari kanan atas kiri, kiri, bawah, kanan, kanan, bawah, bawah, kiri, atas, kiri, bawa,kiri, atas,atas,atas,atas.

t	m	a	j
a	s	a	t
r	a	l	u
a	b	u	a

Cipherteks 1:labjutaaaarmutas
Cipherteks 2:tmajasatraluabua
Contoh pemecahan:
Cipherteks 1:labjutaaaarmutas
Kunci 1:buat 4x4 kotak kosong lalu dari kanan atas tulis melingkar kedalam

10	11	12	1
9	16	13	2
8	15	14	3
7	6	5	4

Arti huruf pertama cipherteks adalah huruf ke 10 plainteks, huruf kedua cipherteks adalah huruf ke 11 plainteks, dan seterusnya.

1.3 *Columnar Transposition Cipher*

Columnar transposition cipher adalah salah satu jenis *transposition cipher* yang sangat mudah dilakukan dan juga dipecahkan, hal ini dilakukan dengan cara mengurutkan huruf per baris dan membacanya kebawah, dalam *cipher* ini kuncinya adalah jumlah huruf per baris. Pemecahan cipher ini bisa dilakukan dengan mudah dengan menebak kunci dengan *bruteforce*.

Contoh:
Plainteks: jam satu aula barat
Kunci 1:4(dibaca kebawah)

j	a	m	s
a	t	u	a
u	l	a	b
a	r	a	t

Kunci 2:5(dibaca kebawah)

j	a	m	s	a
t	u	a	u	l
a	b	a	r	a
t				

Cipherteks 1:jauaatlrmuaasabt
Cipherteks 2:jtataubmaasurala

1.4 *Double Columnar Transposition Cipher*

Double columnar transposition cipher adalah pengembangan dari *columar transposition cipher*. Karena *cipher* tersebut mudah dipecahkan, maka cipher tersebut dilakukan dua kali agar lebih aman. Sebelum diacak lagi urutan kata dimodfikasi terlebih dahulu seperti pembacaan dari belakang atau lain-lain

Contoh:
Plainteks: jam satu aula barat
Kunci 1:4(dibaca kebawah)

j	a	m	s
a	t	u	a
u	l	a	b
a	r	a	t

jauaatlrmuaasabt (dibaca dari belakang) = tbasaaumrltaauaj

t	b	a	s
a	a	u	m
r	l	t	a
a	u	a	j

Kunci 2:5(dibaca kebawah)

j	a	m	s	a
t	u	a	u	l
a	b	a	r	a
t				

jtataubmaasurala(dibaca dari belakang) = alarusaambuatatj

a	l	a	r	u
s	a	a	m	b
u	a	t	a	t
j				

Cipherteks 1:tarabaluautasmaj
Cipherteks 2:asujlaaaatrmaubt

1.5 *Myszkowski transposition*

Myszkowski transposition adalah perkembangan dari columnar transposition cipher dengan menggunakan kunci berupa kata. Dan dari kata tersebut akan diubah ke angka dan digunakan untuk membaca urutan dari *cipher*.Contoh kunci adalah pisang bila diubah bedasarkan urutan di alphabet(a adalah alphabet ke 1, b adalah ke 2 dan seterusnya)pisang= 16, 9, 19, 1, 14, 7. Lalu urutan tersbut akan dibuat peringkat (a adalah peringkat ke 1, sedangkan g adalah peringkat 2)pisang= 5,3,6,1,4,2 lalu hal tersebut akan diubah menjadi urutan pembacaan kolom di *cipher*. Bila terdapat huruf yang sama dalam kunci urutan akan disesuaikan.

Contoh:
Plainteks: jam satu aula barat
Kunci 1:pisang(536142)

5	3	6	1	4	2
j	a	m	s	a	t
u	a	u	l	a	b
a	r	a	t		

Kunci 2:pasang(415132)

4	1	5	1	3	2
j	a	m	s	a	t
u	a	u	l	a	b
a	r	a	t		

Cipherteks 1:slt tb aar aa jua mua
Cipherteks 2:aar slt t baa jua mua

II. GRILLE CIPHER

Grille cipher adalah salah satu cara untuk mengenkripsi pesan, secara umum cara ini berbeda dengan *transposition cipher* dan *substitution cipher*(mengganti huruf dengan huruf atau symbol lain). Akan tetapi beberapa cabang dari *grille cipher* dapat terlihat seperti *transpositional cipher*.

Grille cipher dilakukan dengan menggunakan lembaran(dapat berupa kertas, kardus,kayu, atau bahkan besi) yang memiliki lubang tapi sekarang ini dapat dilakukan dengan bantuan program komputer.

Untuk menyembunyikan pesan dengan *Grille cipher*, dibutuhkan lembaran berlubang untuk menandakan dimana huruf dituliskan.

Lembaran tersebut adalah kunci dari *Grille cipher*. Dengan menggunakan lembaran tetntu saja kunci dari cipher ini akan sulit diketahui orang lain karena tidak berupa kata atau kalimat yang mungkin saja tercuri dengar atau terlihat sekilas. Sehingga satu-satunya cara untuk memecahkan *Grille* adalah memperoleh lempengan.

Terdapat beberapa algoritma *Grille cipher:*

2.1 *Cardan Grille*

Cardan Grille adalah salah satu jenis bentuk *Grille cipher* yang fungsi utamanya adalah untuk menyembunyikan pesan bukan untuk mengengkripsi pesan, sehingga *Cardan Grille* lebih sering digunakan untuk *steganografi*. Untuk melakukan *Cardan Grille* diperlukan lembaran berlubang dan di lubang-lubang tersebut akan diisi huruf, yang diisin dengan pesan lalu setelah itu lembaran tersebut akan diangkat dan diisi dengan kalimat sisanya.

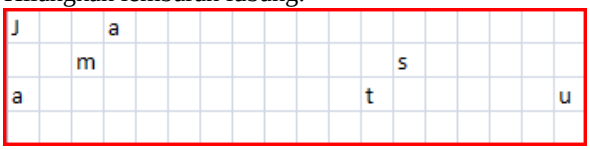
Contoh:

Plainteks: Jam satu

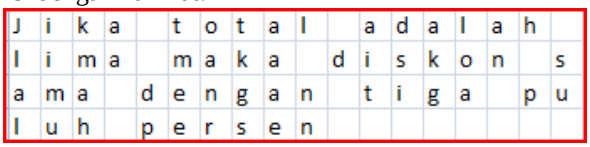
Kunci:

Enkripsi:

Hilangkan lembaran lubang*:*



Isi dengan kalimat:



Keunggulan dari metode ini adalah tidak membutuhkan alat selain lembar berlubang, dan bila ditulis tangan penyembunyian akan lebih mudah karena tidak ada batas huruf yang bisa membatasi.

Contoh:

Dalam kalimat atas kata huruf j dan a pertama dibatasi 2 huruf sehingga bisa ditulis jika, tetapi bila menggunakan tulis tangan orang tidak akan curiga bila terdapat 3 atau 4 huruf dengan cara mengubah ukuran dan bentuk tulisan sebab tulisan tangan orang berbeda-beda, dalam hal ini bisa ditulis ‘jumlah’.

Selain itu dekripsi bisa dilakukan dengan cepat bila pihak yang dituju telah memiliki lembaran, tanpa proses penghitungan.

Dalam metode ini selembar lembar berlubang juga dapat menghasilkan 4 enkripsi yang berbeda dengan cara membalik-balik lembar.

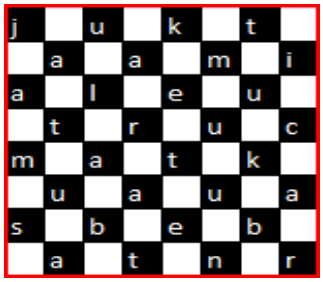
2.1 *Trellis Cipher*

Trellis cipher atau yang disebut juga *chessboard cipher* adalah Grille cipher yang menggunakan pola papan catur sebagai lembar berlubang. Pertama kalimat akan diisi di salah satu jenis warna misal hitam, lalu setalah penuh kalimat akan diisi di warna putih, bila terjadi kekurangan maka sisanya akan diisi dengan huruf asal, bila lebih maka akan digunakan papan lain. Metode ini walaupun terdapat beberapa posisi awal, tidak terlalu aman karena hanya terdapat sedikit kombinasi kunci dibandingkan *cipher* lainnya, dan hanya aman bila kriptanalis(pembongkar enkripsi) tidak tahu bahwa ini adalah *Trellis cipher*.

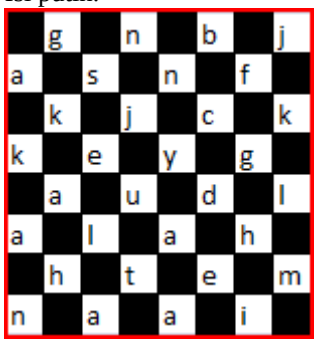
Contoh:

Plainteks: Jam satu aula barat ketemu untuk bicara langkah selanjutnya

Enkripsi: Isi hitam dahulu



Isi putih:



Gabungkan:

j	g	u	n	k	b	t	j
a	a	s	a	n	m	f	i
a	k	l	j	e	c	u	k
k	t	e	r	y	u	g	c
m	a	a	u	t	d	k	l
a	u	l	a	a	u	h	a
s	h	b	t	e	e	b	m
n	a	a	t	a	n	i	r

Cipherteks:jaakmasngaktauhauslealbanajruattkne ytaeabmcuduentfugkhbijikclamr

2.1 *Turnign Grille*

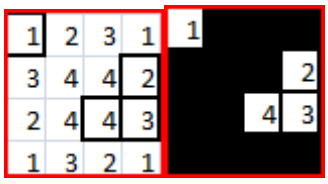
Turning Grille adalah salah satu jenis dimana kuncinya adalah nomor dari blok yang ada. *Grille* ini dibuat dengan cara membuat sebuah papan kotak, dan membaginya menjadi 4. Setalah itu akan diberi nomor di setiap kuadran penomoran pada kuadran dilakukan dengan cara merotasi tiap kuadran.

Contoh:

1	2	3	1
3	4	4	2
2	4	4	3
1	3	2	1

Setelah itu akan dipilih nomor yang akan dijadikan kotak untuk mengisi. Setiap nomor harus dipilih dan setiap nomor hanya bisa dipilih sekali:

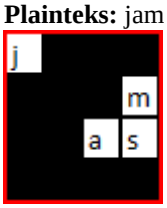
Contoh:



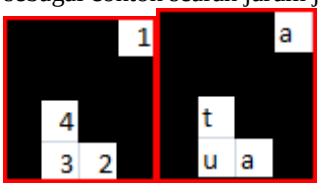
Lalu huruf akan diisi bedasarkan nomor yang telah dipilih.

Contoh:

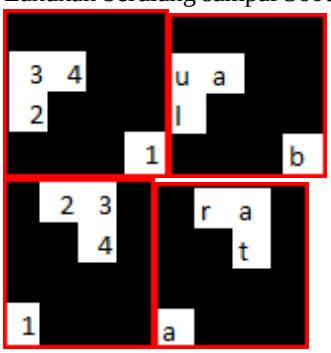
Plainteks: jam satu aula barat



Lalu putar (boleh searh jarum jam atau berlawanan) sebagai contoh searah jarum jam dan isi



Lakukan berulang sampai 360derajat



Satukan:

j	r	a	a
u	a	t	m
l	a	s	t
a	u	a	b

Cipherteks:julaaauatsaamtb

III. PENGUJIAN METODE TRANSPOSISI

Dalam kriptografi ada beberapa hal yang perlu diperhatikan dalam pengenkripsian:

1 Enkripsi mudah digunakan oleh pengirim dan penerima.

2 Pesan tidak dapat dimengerti oleh orang yang bukan tujuan

3 Pesan tidak terlihat atau tidak diketahui keberadaanya oleh orang yang bukan tujuan(lebih kearah steganografi, sehingga tidak wajib di kriptografi)

Untuk hal itu akan diuji ke beberapa orang yang memiliki kondisi sama tentang *cipher-cipher* diatas. Pengujian akan dilakukan 3 tahap.

1 Menanyakan apakah mengerti pesan yang terenkripsi dengan memberikan informasi tentang cipherteks dan diberitahukan metode apa yang digunakan dan mengukur apakah bisa ditemukan

jawabannya dan diukur waktunya.(menguji keamanan)

2 Menanyakan arti dari pesan dengan memberikan kunci serta cara memecahkannya dan menghitung waktu pemecahannya. (menguji kemudahan pemakaian bagi penerima pesan)

Untuk poin ketiga tidak dilakukan percobaan karena tingkat ketersembunyian *transposition cipher* tidak ada karena pesan terlihat aneh.

Untuk metode *Grille* tidak akan dilakukan karena mustahil memecahkan kode tanpa kunci dan bila mendapat kunci akan menjadi snagat mudah dan cepat. Tingkat keamanan juga berbanding lurus dengan kompleksitas *Grille*. Untuk *Cardan Grille*, tingkat ketersembunyian pesan juga sangat tinggi. Sedangkan untuk *Grille* lain yang disebutkan diatas tidak memiliki ketersembunyian.

Untuk pengujian tahap pertama akan dibatasi dengan waktu 15 menit, bila lebih dari itu maka teks dianggap aman. Untuk tahap dua akan dibatasi waktu 5 menit bila lebih maka akan dianggap sulit digunakan.

Telah dilakukan pengujian oleh 3 orang yang telah diberi pengarahan tentang metode-metode tersebut. Berikut data-data mengenai hasil pengujian metode enkripsi:

Soal yang digunakan adalah:

1.

Metode	*Rail Fence*
Cipherteks	ttniakaaankemnugad
Kunci	4
Plainteks	Tingkat keamanan dua

2.

Metode	*Rail Fence*
Cipherteks	aaapbriaadnku
Kunci	4
Plainteks	Apa kabar dunia

3.

Metode	*Route*
Cipherteks	usehggnagnarnimi
Kunci	Kotak 4x4 melingkar dari kanan atas ke bawah dalam
Plainteks	Hari minggu senang

4.

Metode	Route
Cipherteks	suksguainkaaayap
Kunci	Kotak 4x4 melingkar dari kanan atas
Plainteks	Siapa yang suka aku

5.

Metode	*Columnar*
Cipherteks	arreyiinaccamaak
Kunci	4
Plainteks	Ayam rica rica enak

6.

Metode	*Columnar*
Cipherteks	ignpkoguartnneeg
Kunci	4
Plainteks	Ikan goring tepung

7.

Metode	*Double Columnar*
Cipherteks	punikbarptaudu
Kunci	6
Plainteks	Buka pintu dapur

8.

Metode	*Double Columnar*
Cipherteks	uapkrpkiemsge
Kunci	6
Plainteks	Pergi ke kampus

9.

Metode	*Myszkowski*
Cipherteks	alaksakudrius
Kunci	Baca
Plainteks	Kalkulus dasar

10.

Metode	*Myszkowski*
Cipherteks	imostnmsirisefa
Kunci	Baca
Plainteks	Sistem iformasi

Hasil dari pengujian adalah:

1. Penguji nomor 1

No.	Tahap 1	Tahap 2
1	Gagal	232 detik
2	Gagal	242 detik
3	Gagal	17 detik
4	Gagal	15 detik
5	74 detik	Tidak dilakukan
6	87 detik	Tidak dilakukan
7	Gagal	272 detik
8	Gagal	105 detik
9	Gagal	Gagal
10	Gagal	194 detik

2. Penguji nomor 2

No.	Tahap 1	Tahap 2
1	Gagal	Gagal
2	Gagal	Gagal
3	Gagal	Gagal
4	Gagal	Gagal
5	62 detik	Tidak dilakukan

6	45 detik	Tidak dilakukan
7	Gagal	Gagal
8	Gagal	Gagal
9	Gagal	93detik
10	Gagal	85 detik

3. Penguji nomor 3

No.	Tahap 1	Tahap 2
1	Gagal	165 detik
2	Gagal	98 detik
3	Gagal	240 detik
4	Gagal	17 detik
5	25 detik	Tidak dilakukan
6	20 detik	Tidak dilakukan
7	Gagal	47 detik
8	Gagal	121 detik
9	Gagal	232 detik
10	Gagal	53 detik

IV. PERHITUNGAN DAN ANALISIS

Hasil pengujian yang didapat terdapat beberapa anomaly seperti pada kasus penguji pertama rata-rata waktu yang dipakai untuk memecah soal lebih lama daripada yang lain. Hal ini mungkin disebabkan keadaan penguji satu yang kurang konsentrasi. Untuk penguji dua kegagalan pada beberapa soal di tahap 2 mungkin disebabkan kurang mengerti metode dari enkripsi sola-soal tersebut. Dan pada pengujian di penguji 3 tampak hasil yang cukup baik walaupun terdapat data yang cukup aneh yang mungkin disebabkan oleh faktor kondisi lingkungan.

Data yang didapat memang hanya didapat dari sample yang sedikit. Hal ini disebabkan kurangnya waktu dan sukarelawan untuk menjadi penguji. Data memang tidak 100% representatif tapi akan dijadikan acuan untuk analisis.

Berikut rata-rata dari waktu setiap metode enkripsi bedasarkan hasil uji diatas:

Metode	Tahap1	Tahap2
Rail fence	Gagal	184.25
Route	Gagal	72.25
Columnar	52.17	0
Double columnar	Gagal	136.25
Myszkowski	Gagal	131.4

Dilihat dari rata-rata diatas dapat diperoleh kesimpulan bahwa *columnar cipher* mempunyai tingkat keamanan yang sangat rendah karena hanya membutuhkan waktu sebentar untuk memecahkannya tanpa kunci. Selain itu metode lain cukup aman untuk digunakan.

Dilihat dari rata-rata, urutan kemudahan dari metode *transposisi*, memiliki urutan sebagai berikut:

1. Columnar
2. Route
3. Myszkowski
4. Double Columnar
5. Rail Fence

Akan tetapi bila dibandingkan dengan panjang kunci, metode ini yang memberikan kemudahan dalam penyampaian pesan:

1. *Rail Fence*
2. *Columnar*
3. *Double Columnar*
4. *Myszkowski*
5. *Route*

Dari banyak langkah-langkah pemecahan dan enkripsi:

1. *Columnar*
2. *Rail Fence*
3. *Route*
4. *Myszkowski*
5. *Double Columnar*

Bila diberi poin (1 untuk peringkat bawah dan 5 untuk peringkat pertama) untuk masing-masing panjang kunci, keamanan, waktu pemecahan, dan jumlah langkah memecahkan:

Metode	Panjang kunci	Waktu	Langkah	Total
Rail Fence	5	1	4	10
Route	2	4	3	9
Columnar	4	5	5	14
Double Columnar	3	2	1	6
Myszkowski	1	3	2	6

Berikut peringkat saran penggunaan metode yang ada:

1. *Rail Fence*
2. *Myszkowski*
3. *Double Columnar*
4. *Route*(Kunci terlalu panjang)
5. *Columnar*(tidak aman)

Untuk metode Grille yang memiliki tingkat keamanan yang paling tinggi adalah Cardan Grille karena kunci tidak memiliki pola dan pesan tersembunyi. Sedangkan metode lain dapat diketahui dengan mudah bila tahu metodenya.

V. SARAN UNTUK MEMPERLUAS PENGGUNAAN METODE TRANSPOSISI DAN GRILLE

Berikut beberapa saran untuk memperluas berbagai metode tanpa mengubah panjang kunci, mempersulit kuncinya dan memperbanyak langkah secara signifikan..

1. *Rail Fence*:digabungkan dengan metode *caesar chipher*. Metode subtitusi lain akan memperpanjang kunci. Penggabungan dengan metode *columnar* memungkinkan, akan tetapi penggabungan dengan metode transposisi lain akan membuat kunci panjang dan langkah dekripsi/enkripsi meningkat signifikan.

2. *Route* :Bisa digabungkan dengan berbagai metode *columnar* dan *double columnar*. Metode subtitusi yang cocok digabung adalah vigenere atau *auto-key vigenere*. Akan tetapi tidak terlalu cocok karena rute kunci bisa direpresentasikan dengan berbagai bahasa: contoh: ‘dari kanan atas melingkar’ dengan ‘ melingkar dari kanan atas’ akan menghasilkan *vigenere* yang berbeda.

3. *Columnar:* Tidak aman, cocok untuk diubah menjadi *double columnar* atau *Myszkowski*. Dapat digabung dengan *Caesar cipher*.

4. *Double Columnar:* dapat digabung dengan *Rail Fence*, untuk metode subtitusi cocok dengan *Caesar cipher.*

5. *Myszkowski*:Dapat digabung dengan *Rail Fence* dengan kunci dari panjang kunci *Myszkowski*. Untuk metode subtitusi dapat digabung dengan berbagai metode seperti *vigenere, auto-key vigenere, Caesar cipher, playfair,* dan berbagai metode lain.

6. *Cardan Grille*: Digabungkan dengan metode transposisi dan subtitusi diperlukan pembentukan kunci baru, tetapi bisa dilakukan dengan cara seperti emnghitung jumlah lubang untuk kunci berupa angka, tetapi tidak adaptif untuk lempengan non-elektronik. Dapat digabung dengan diri sendiri untuk memperbanyak kata yang dapat ditulis. Contoh:Menulis seperti biasa dengan satu sisi lempengan lalu lempengan tersebut diputar bila ingin menambah kata. Penggunaan prinsip rotasi untuk memperbanyak masukan kata juga dapat dilakukan.

7. *Trellis Grille:* Digabung dengan *columnar* dengan pnajang kololm sesuai panjang papan, digabung dengan *Caesar cipher* dengan panjang kunci sesuai panjang papan dan berbagai metode lainyang menggunakan kunci angka, tidak efektif bila panjang papan yang digunakan tetap.

8. *Turning Grille:* seperti *Trellis* dapat digabungkan dengan berbagai metode dengan kunci panjang papan, akan tetapi juga tidak terlalu efektif. Penggunaan papan berukuran ganjil dapat mmeningkatkan efisiensi *Grille.* Meratan jumlah angka yang dipilih per kuadran dapat mengingkatkan efektifitas *Turning Grille.*

Secara umum berbagai metode dapat dilakukan pada metode-metode di atas, seperti penulisan *cipher* yang tidak dimulai dari awal pembacaan yang dilakukan dari sudut yang berbeda. Diubah ke bahasa asing. Diubah menjadi iymbol seperti bit dan morse sebelum dienkripsi. Disembunyikan dengan metode steganografi dan masih banyak lagi.

VI. KESIMPULAN

1. Terdapat berbagai metode *transposition cipher*, dengan tingkat keamanan dan kemudahan yang berbeda-beda

2. Terdapat berbagai metode *Grille* yang berbeda-beda, dengan tingkat keamanan sangat tinggi dan dapat digunakan sebagai steganografi

3. *Grille* sangat aman bila kuncinya tidak diketahui orang lain, bahkan kunci sulit untuk dibuat ulang.

4. Metode *Rail Fence* dan *Myszkowski* sangat baik untuk digunakan dibanding *transposition cipher* lain.

5. Terdapat berbagai cara untuk memperluas penggunaan *transposition* cipher dan *Grille cipher.*

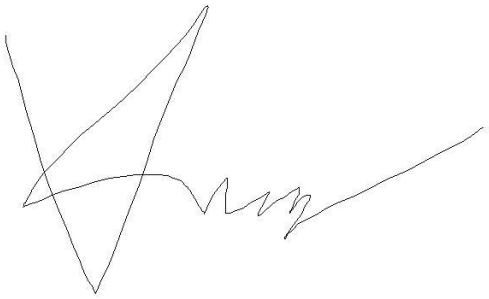
REFERENCES

[1] http://en.wikipedia.org/wiki/Transposition_cipher
[2] http://en.wikipedia.org/wiki/Grille_%28cryptography%29

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 19 Maret 2012



Kevin Wibowo/13509065